Manuscript Details

Manuscript number	IJMI_2018_966_R1
Title	Evaluating Information Security Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector
Article type	Research paper

Abstract

Background: The numbers of reported public sector information security incidents has significantly increased recently which includes a 22% related to the UK health sector. Over two thirds of these incidents pertain to human error but despite this there are limited published related works researching human error as it affects information security. Method: This research conducts an empirical case study into the feasibility and implementation of the Information Security Core Human Error Causes (IS-CHEC) technique which is an information security adaptation of Human Error Assessment and Reduction Technique (HEART). We analysed 12 months of reported information security incidents for a participating public sector organisation providing healthcare services and mapped them to the IS-CHEC. Results: The results show that IS-CHEC is applicable to the field of information security but identified that the underpinning HEART human error probability calculations did not align to the recorded incidents. The paper then proposes adaptation of the IS-CHEC technique based on the feedback from users during the implementation. We then compared the results against those of a private sector organisation established using the same approach. Conclusions: The research concluded that the proportions of human error are far higher than previously reported current literature. The most common causes of human error within the participating public sector organisation were lack of time for error detection and correction, no obvious means of reversing an unintended action and people performing repetitious tasks.

Keywords	Information Security, Human Error Assessment and Reduction Technique (HEART), Information Security Core Human Error Causes (IS-CHEC), Human Error Related Information Security Incidents, Human Reliability Analysis (HRA)
Taxonomy	Computer Security and Privacy, Computer Security

Corresponding Author	Ying He
Corresponding Author's Institution	De Montfort University
Order of Authors	Mark Evans, Ying He, Iryna Yevseyeva, Leandros Maglaras, Helge Janicke

Submission Files Included in this PDF

File Name [File Type]

RESPONSE LETTER for IJMI_2018_966_final.docx [Response to Reviewers]

Highlights.docx [Highlights]

Public Sector Results and Comparison Article 05-01-2019.docx [Manuscript File]

CONFLICT OF INTERESTS.docx [Conflict of Interest]

AUTHOR DECLARATION.docx [Author Statement]

SUMMARY Table.docx [Supporting File]

To view all the submission files, including those not included in the PDF, click on the manuscript title on your EVISE Homepage, then click 'Download zip file'.

Evaluating Information Security Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector

Mark Evans, Ying He *, Leandros Maglaras, Iryna Yevseyeva, Helge Janicke

Cyber Security Centre, De Montfort University, England

Abstract

Background: The numbers of reported public sector information security incidents has significantly increased recently which includinges a 22% related to the UK health sector. Over two thirds of these incidents pertain to human error, but despite this, there are limited published related works researching human error as it affects information security.

Method: This research conducts an empirical case study into the feasibility and implementation of the Information Security Core Human Error Causes

(IS-CHEC) technique which is an information security adaptation of Human Error Assessment and Reduction Technique (HEART). We analysed 12 months of reported information security incidents for a participating public sector organisation providing healthcare services and mapped them to the IS-CHEC technique.

Results: The results show that the IS-CHEC technique is applicable to the field of information security but identified that the underpinning HEART human error probability calculations did not align to the recorded incidents. The paper then proposes adaptation of the IS-CHEC technique based on the feedback from users during the implementation. We then compared the results against those of a private sector organisation established using the same approach.

Conclusions: The research concluded that the proportions of human error isare far higher than previously reported in current literature. The most common causes of human error within the participating public sector organisation were lack of time for error detection and correction, no obvious means of reversing an unintended action and people performing repetitious tasks.

Key words: Information Security, Human Error Assessment and Reduction Technique (HEART), Information Security Core Human Error Causes (IS-CHEC), Human Error Related Information Security Incidents, Human Reliability Analysis (HRA)

1. Introduction

The number of incidents reported to the Information Commissioner's Office (ICO) by a number of UK sectors increased significantly from July to September 2017 [1] in comparison to published figures for April to June 2017. ~~Some of t~~These sectors included the health sector which increased by 22% and continues to be the sector with the highest percentage of data breaches [2], the education sector with an increase of 68% and ~~a staggering increase of 178% pertaining to~~ the central government sector with a staggering increase of 178%. Within the health sector, the main breach types were data posted or faxed to an incorrect recipient, data sent via email to an incorrect recipient and loss or theft of paperwork. Incident reporting is a core component of the National Health Service in the United Kingdom [3].

The NHS Digital Information Security Incident Good Practice Guide [4] acknowledges that losses of personal data are damaging to the person concerned and the NHS as a whole. The document ~~and~~ [4] even lists 'human error such as emailing data by mistake' as an example of an information security incident. However, ~~it~~ within the document [4] it does not expand on human error related to the email example above or the probable causes in terms of richer information. ~~and t~~Therefore there is no published guidance within the document on how to understand and prevent human error from occurring. Human errors including slips, lapses and negligence have~~as~~ been

acknowledged in the literature as common reasons that information security incidents occur [5–8]. ~~Organisational data breaches can occur in a number of ways with cyber attacks being the most reported form of data breach, but malicious insiders and employee negligence being the biggest risk [9].~~ It is expected that the actual volumes and types of breaches will be better known and understood from May 2018. The General Data Protection Regulation (GDPR) introduced a duty on all organisations to report personal data related breaches and incidents to the ICO within 72 hours of becoming aware of themit [9]. This shouldwill result in richer information being published by the ICO.

A recent study [10] estimated that there was an average probability of 27.7% that organisations participating in the study would suffer a data breach within the next 24 months. It was also presented that the average cost of data breaches that were as a result of human error or negligence was $126 per record. It was also established that the mean time to identify a human error related data breach was 168 days and the mean time to contain the breach was 54 days.

It was recently publishedestablished that UK local authorities suffered in excess of 98 million cyber attacks since 2017 [9] which equates to 37 attempted breaches every minute. It was also confirmed that at least one in four councils experienced an actual security breach in this time. Cyber attacks are designed to exploit humans who are perceived to be the weakest cyber security link [9] and it is suggested all local authority staff should have

basic cyber security awareness. This suggestion is very much focused upon the mitigation for intentional malicious attacks that exploit humans but does not address the issue of ~~underlying non-malicious activity~~unintentional~~,~~ human error which~~, that~~ results in the majority of information security incidents and breaches [11]. It has been published in our previous work that the majority of information security incidents and breaches are as a result of human error but that this is in fact the consequence of organisational failings rather than the cause [12].

It has been found that many breaches occur due to some form of human error [13] and that between April 2011 and April 2014 there were 4,236 UK local authority breaches. These breaches included 628 cases of i~~l~~ncorrect or inappropriate data being shared on emails, letters and faxes, 401 cases of data loss or theft, 159 cases of data being shared with a third party~~,~~ and 99 cases of unauthorised people accessing or disclosing data.

This research follows on from our previous research where we applied the IS-CHEC technique, formerly known as HEART-IS, in the same way to analyse the same 12 month period of reported information security incidents within a private sector organisation. The name of the technique was changed upon discussion with the original creator of the HEART technique to clearly distinguish between the original HEART technique and IS-CHEC, as well as intellectual property.

This research conducts an empirical case study into the feasibility and implementation of the Information Security Core Human Error Causes (IS-

CHEC) technique which is an information security adaptation of Human Error Assessment and Reduction Technique (HEART). We analysed 12 months of reported information security incidents for a participating public sector organisation and mapped them to the IS-CHEC technique. This would enable us to understand if the IS-CHEC technique is feasible to the public sector in terms of information security incident management and associated qualitative and quantitative elements, such as the calculated HEART human error probability compared to actual incident likelihood. Finally a comparison of results will be undertaken against private sector results [12].

This paper makes the following contributions:

- Conducts an empirical case study to investigate the feasibility of applying the Information Security Core Human Error Causes (IS-CHEC) technique within a public sector information security setting for the first time in the literature.
- Presents an empirically validated understanding into the proportions and causes of human error related information security incidents within a public sector organisation.
- Proposes further adaptation of the IS-CHEC technique and tool based upon a comparison of case study findings within public and private sector organisations.
- Validates the empirical case study results against published public sector personal data breaches and incidents.

This paper presents the findings of an empirical case study into the feasibility and implementation of the Information Security Core Human Error Causes

(IS-CHEC) technique. The case study comprisesing of a retrospective analysis of twelve months of reported information security incidents within a public sector participating organisation. The case study findings will be compared to our previous research [12] relating to the same research that was undertaken within a private sector organisation. Following on from our previous research [11], this paper forms an element of wider study whereby the validated results from the empirical study will form the basis of informed likelihood calculations to ensure the predictive element of HEART is applicable to the field of information security. The results of this public sector case study and the previous private sector case study enabled us to present adaptations to the HEART HRA technique in the form of the IS-CHEC tool and technique and tool which is applicable to, and reflects, information security practices.

The remainder of this paper is structured as follows. Section 2 presents related work. Section 3 details the research method including the case study organisation and introduces the IS-CHEC technique. Sections 4 and 5 present the IS-CHEC technique and tool utilised to conduct the empirical research and proposed adaptations. Sections 6 and 7 present the detailed results of the case study and comparison with the private sector. Sections 8 and 9 provide the findings, implications of the research, comparison and validation against published literature and personal data breaches, conclusions and outline planned future work.

2. Related Work

Current human factors information security research places an imbalanced focus on intentional actions rather than unintentional human error [14]. Published information systems human behavior related research predominantly addresses the problem of intentional violations and non-compliances [15–39] resulting in proportionally limited work relating to unintentional human error [40–42]. Therefore there are limited published related works researching human error as it affects information security. Published research appears to be ~~be focused on~~ theoretical using techniques such as~~elements and~~ surveys [43] rather than empirical validation based on techniques including interviews or action research and case studies as set out within our research. As a result, there are diverse understandings on the actual proportion and volumes of incidents relating to human error. As stated in our previous research [11], the majority of incidents pertain to human error and this was supported in the empirical research we conducted within a private sector organisation [12]. As examples of this, the work presented by Hamid et al [44] states that human errors add a 39% contribution to the information security incidents experienced by organisations, and Wall [45] found that published data suggested that 47% of breaches were due to insiders and of this figure 31% related to human error. We argue that this figure is proportionally lower than actual exposure as expressed within this paper and previous empirical validation [12]. In support of our research, Parsons et al [46] identified as part of their work that human error was a factor in 95%~~5 percent~~ of information security incidents.

Published works present a general understanding that humans are the

weakest information security link [43,46–49], the main threat [48], and that human characteristics commonly lead to most information security breaches [46,48,50]. Basin, Radomirovic and Schmid [51] emphasise that many business practices rely upon humans and that humans are computationally weaker than machines as they can be naïve, careless or gullible. Human error related information security incidents can occur where a person is completing an intended activity but performs an unintentional action caused by human characteristics such as negligence and carelessness [43,48]. However such incidents can also occur as a result of targeted attacks exploiting specific human weakness [49]. Mahfuth et al [48] point out that on one hand humans are, and create, threats to an organisation but on the other hand are key in protecting against or preventing incidents and breaches. Research has identified that an effective information security culture can lead to employees acting as a 'human firewall' safeguarding information and that despite the application of technical security approaches, this is not enough as information security is both a technical and people issue [52–54]. For the information security community and organisations to focus their~~its~~ attention on technical measures to protect information without consideration of the human factor is inadequate [48]. Information security is primarily a human factors problem that remains unaddressed and on~~as in~~ many occasions organisations overlook the human factor [47].

Detecting and preventing the insider threat and associated risk is complex and difficult to mitigate [55]. Insiders reside within organisational defences and often have elevated privileges to infrastructure, systems and data [55]

and therefore managerial security, as opposed to technical security, is vital [50]. In order for an organisation to identify vulnerabilities in its systems or processes that could be exploited by humans it is important that they examine and understand all possible human error causes [56].

Research has also found that there are gaps in current information security practice with regard to the human factor, including behaviour and error which have not been explored [44] or given attention within literature [47]. Furnell et al [43] stated that people are often not provided with adequate guidance to enable effective information security decisions and Hwang and Cha [57] also added that for most employees, achieving their own job goal is the priority and information security may be a hindrance or even cause conflict. AlHogail [52] indicated that although researchers have addressed the role of human behaviour within information security, there is little evidence of the application of this knowledge.

As set out within our earlier work [12], it is essential for the information security community to fully understand the types and causes of human error in order for it to be treated effectively. As set out by James Reason [58], human error comprises of a number of fundamental elements. These elements include that human error can only be as a result of an intended action not achieving their desired outcome, and comprises of a greater degree of granularity than is currently applied and published. A human error could be as a result of a slip~~s,~~ (an incorrect action which is associated with a correct intention [59]), a lapse~~s,~~ (forgetting to do something~~,~~ or losing your place

midway through a task [60]),~~,~~ or a mistake~~s,~~ (a failure of intended actions to achieve their desired outcome [58]). Mistakes are then broken down into rule-based or knowledge-based mistakes. Rule-based mistakes can occur if an incorrect rule is used [61] perhaps as part of an organisational policy or procedure~~s,~~ whereas knowledge-based mistakes occur where there is a lack of rules or procedures resulting in a human having to make a quick decision [61]. All of the above mentioned human error categories could potentially be caused by human error relating to people at both the sharp or blunt end but they could also be the consequences of organisational deficiencies including poor working environment, lack of resources (including time), or a lack of, or inadequate, policies and procedures. It is also set out by Reason [58] that different cognitive stages can be applied. Mistakes would be as a result of the planning stage whereas lapses would be as a result of the storage phase and slips relate to the execution stage. Human errors would not include violations~~,~~ defined as deliberately doing the wrong thing. Reason [62] sets out that the human error problem can be viewed as either through the person approach or system approach~~es~~ which has a different model of error causation. The person approach focus~~s~~es on human fallibility and blames the~~hem~~ person for errors including forgetfulness and inattention. ~~whereas~~ Alternatively, the system approach accepts that humans are fallible and that errors are consequences rather than the cause and applies the principle that the human condition cannot be changed but the conditions under which humans work can.

3. Methodology

3.1 Case Study Organisation

The case study organisation is a public sector organisation which provides healthcare services. It has approximately 2000 employees and provides a range of services and its incident management practices are required to support compliance with legislation and government guidance. The participating organisation was selected through opportunity and agreement with the parent university. Information security is governed centrally by the Head of Information Security and their small team who are responsible for the development of organisational strategy and policy as well as oversight and engagement in all reported incidents. Designated individuals, usually managers, within each business area have responsibility for information security application in addition to their primary role. These Business area representatives are not dedicated information security professionals but attend formal governance sessions with the information security team on a bi-monthly basis. The organisation has an information security policy as well as an information security incident policy and procedures in place which are communicated to all employees as part of annual awareness requirements. Compliance in terms of awareness are continuously monitored and acted upon.

We conducted an empirical study using the IS-CHEC technique to perform a retrospective analysis of recorded information security incidents within the participating public sector organisation. We applied the IS-CHEC technique to capture and analyse recorded incidents in order to establish those that

related to human errors and if the tasks and associated error producing conditions could be mapped and established. The analysis was undertaken on all information security incidents recorded between 1st June 2015 and 31st May 2016. The case study ~~was a longitude study, which~~ spanned a duration of approximately ten months.

3.2 Case Study Method

In order to conduct the empirical study, the IS-CHEC (Originally called HEART - IS) technique~~method~~ and tool was used as presented in our previous study within a private sector organisation [12]. The IS-CHEC technique is an adapted version of the HEART technique that is split into two elements which can be seen in the appendices. These are an IS-CHEC mapping element and an analysis element. The mapping element was appended to the participating organisation's incident register to enable all recorded incidents to be analysed against HEART in terms of its components such as generic task types (GTT) and error producing conditions (EPC). A number of additional fields were also created to enable the collection of associated information that we believed would add value to both the research and~~but~~ also the participating organisation due to gaps in current published information security literature. The added fields enabled us to capture the common types of activities and roles associated with incidents which we feel are missing in related work and research. The IS-CHEC analysis element was a separate tool from the mapping tool which comprised of a number of

fields, which were used in order to allow the HEART in-built likelihood calculations to be analysed against actual incident likelihoods.

4. Implementation of IS-CHEC

The incident data collection, IS-CHEC mapping and analysis, and reporting steps were undertaken throughout the course of the case study and are expanded upon below.

4.1 Incident Data Collection

In order to ensure that the recorded information security incidents for all business areas within the participating organisation were validated based upon greater local business knowledge, it was essential that local business area leads were engaged for each business area. The retrospective incident analysis was performed on 322 incidents reported between 1/6/2015 and 31/5/2016. 322 (100%) of incidents and mapping data were confirmed as being validated by the respective business area leads.

The next step was to obtain an anonymised incident register securely from the participating organisation covering the period from 1st June 2015 to 31st May 2016 which would be the core data set analysed. The incident register contained basic details of all incidents reported during this period.

It was also decided as part of the case study to capture the primary element of the role being performed that was being undertaken when the incident occurred. The participating organisations were provided with the primary element of the role options below:

- Administration

- Communications
- Computer End User
- Data Entry
- Filing
- Email User
- Human Resources
- IT Support
- Line Manager
- Mobile Phone User
- Mobile Computer User
- Mobile Computing Device User
- Senior Management
- Remote/Home Worker
- Document or Equipment Destruction

4.2 Implementing the IS-CHEC mapping element

The IS-CHEC mapping element, as shown in table A2 with-in the appendices, was originally presented in our private sector research [12] and comprised of core HEART components such as GTT, EPC and Associated Proportion of Affect (APOA) to enable the population of associated HEART data and associated research analysis. An amendment from the standard HEART approach was to utilise the use of percentages rather than decimals to capture the APOA for each EPC as it was felt that this would aid understanding due to literature stating a weakness of HEART is the subjective nature of determining the APOA [63]. We provided the tool to each business area representative to enable them to establish required HEART data for each

reported incident to address previous literature which stated that assessors found the population of the APOA difficult.

In accordance with the HEART User Manual [59], a conservative approach was applied. This approach only includes ~~only~~ an EPC if it definitely was a factor in the incident occurring and also utilising a lowest defined value for the APOA. In order to enable accurate probabilistic calculations to be obtained, the participating organisation was only able to select up to a maximum of 3 EPCs for each incident.

4.3 Implementing the IS-CHEC analysis element

The intention of the IS-CHEC analysis element [12] was to enable data analysis of the inbuilt HEART likelihood calculations. The IS-CHEC analysis element captured HEART in-built values including the nominal, lower and higher unreliability bounds associated with each GTT, the strength of each identified EPC, automated calculation fields to determine the nominal likelihood of failure~~,~~ and also fields to capture actual numbers of incidents in order to determine the actual likelihood of incidents that were experienced by the organisation.

We fully populated the IS-CHEC analysis element based upon the data provided by the participating organisation. In addition, it was necessary to review all reported incidents and group them to understand the actual number of times that a specific type of incident occurred in order to ascertain actual frequency of occurrence. This included understanding the tasks and activities that were being performed as well as reviewing the incident description to establish the volumes of repeated incidents.

4.4 Final data analysis and reporting

Finally the complete IS-CHEC data set was analysed manually and through use of IBM SPSS software. Once the analysis was completed, a report was compiled for the participating organisation in order for them to have sight of the full results of the feasibility study. The details of ~~which~~ the results are included within the results analysis section of this article.

5. Adaptation of IS-CHEC

It was found that the HEART GTT descriptions contained not only the type of task but also the environmental context. Therefore, in order to make the incident mapping consistent, the GTTs were mapped to the captured specific tasks and renamed to General Information Security Affecting Tasks (GISAT). Therefore, people capturing incident data can easily map the incident to a specific task such as sending an email rather than distinguishing between complex GTT descriptions. The mapping can be seen in table 1. Following analysis of wider incident data published by the ICO, two further GISATs were recorded relating to faxing of information and sharing in person to ensure the technique and tool are comprehensive.

GISAT	HEART GTT Mapping	Mapping based on retrospective incident analysis within private and public sector organisations
GISAT1- Sending an email	G	A, D, G
GISAT2 - Entering, updating or deleting data within a system, file or document	D	B, D, E, F, G, H
GISAT3 - Posting an item or information	E	E, G
GISAT4 - Configuring a system	B	B, D, F
GISAT5 - Administering a system	D	B, D, E
GISAT6 - Scanning a document	E	E
GISAT7 - Printing a document	E	B
GISAT8 - Providing information verbally	G	D, E, G
GISAT9 - Delivering information or equipment	D	D
GISAT10 - Filing or sorting information	E	B, D, E, G
GISAT11 - Reading or checking an email, file, document or item	G	-
GISAT12 - Safeguarding information or	D	A, D, E, M

GISAT	HEART GTT Mapping	Mapping based on retrospective incident analysis within private and public sector organisations
equipment		
GISAT13 – Destroying information or equipment	D	D
GISAT14 – Accessing a location or environment	G	D, E, G
GISAT15 – Faxing information	E	-
GISAT16 - Sharing or handing over information or equipment in person	G	-

Table 1 – Mapping of IS-CHEC General Information Security Tasks (GISAT) to HEART GTTs

Next, in order to aid understanding by all involved in the investigation of human error information security incident causes, the term Error Producing Condition (EPC) has been changed to Core Human Error Cause (CHEC). Two additional CHECs have been added. These relate to little or no self-checking or testing of output as identified in our previous research [12] and also a lack of significant job aids as captured within HEART GTT G.

In order to support greater understanding and usability in relation to the APOA, the naming convention was again amended to become the CHEC

Weighting or Significance (WoS). Also, in order to address the issue of users 'over scoring' the HEART APOA the graphical rating scale, ranges and rules set out in table 2 are applied to the IS-CHEC technique to prevent weighting exceeding 1.0.

<table>
<tr><th colspan="2">WoS Graphical Rating Scale</th><th>WoS Ranges and Rules</th></tr>
<tr><td>1.0</td><td>Entirely the cause of the error</td><td rowspan="10">Most significant CHEC WoS
Range: 0 - 1.0

Second most significant CHEC WoS
Range : 1.0 minus Primary CHEC WoS
Rule: Cannot exceed Primary CHEC WoS

Least significant CHEC WoS
Range: 1.0 minus (Primary CHEC WoS + Secondary CHEC WoS)
Rule: Cannot exceed Secondary CHEC WoS</td></tr>
<tr><td>0.9</td><td></td></tr>
<tr><td>0.8</td><td rowspan="2">Significant cause of the error</td></tr>
<tr><td>0.7</td></tr>
<tr><td>0.6</td><td></td></tr>
<tr><td>0.5</td><td>Moderate cause of the error</td></tr>
<tr><td>0.4</td><td></td></tr>
<tr><td>0.3</td><td rowspan="2">Insignificant cause of the error</td></tr>
<tr><td>0.2</td></tr>
<tr><td>0.1</td><td></td></tr>
</table>

WoS Graphical Rating Scale		WoS Ranges and Rules
0	Not a cause of the error	

Table 2 – CHEC Weighting or Significance (WoS)

The IS-CHEC model to be applied to information security incident management is presented in figure 1. This is a lower-level adaptation of the plan-do-study-act model presented in our previous research [11].

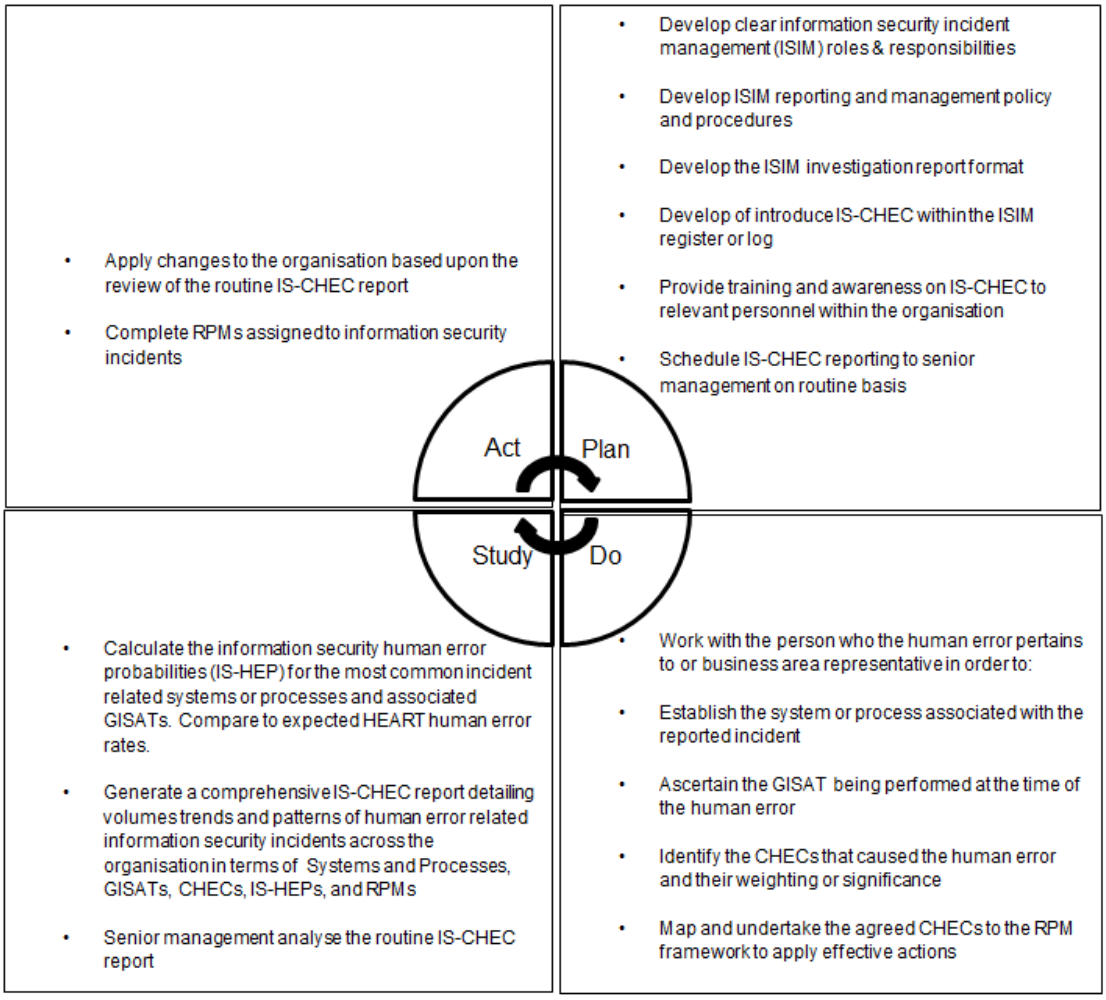

Figure 1 – IS-CHEC Incident Management Model

6. Results

The following sections of the report present the findings of the retrospective incident analysis for the participating public sector organisation.

6.1 General Results

The participating organisation analysis identified that 298 (92.5%) of the 322 reported and validated incidents were due to human error as shown in table 3. This is in line with the volumes presented by Parsons et al [46].

		Due to Human Error (y/n)		
		N	**Y**	**Total**
Organisation Area	Organisation Area M	2	3	5
	Organisation Area N	1	1	2
	Organisation Area O	0	8	8
	Organisation Area P	0	3	3
	Organisation Area Q	7	12	19
	Organisation Area R	3	41	44
	Organisation Area S	0	1	1
	Organisation Area T	3	80	83
	Organisation Area U	1	25	26
	Organisation Area V	0	3	3
	Organisation Area W	0	75	75
	Organisation Area X	7	43	50
	Organisation Area Y	0	2	2
	Organisation Area Z	0	1	1
Total		24	298	322

Table 3 – Human error related incidents

256 incidents (87.7%) of the validated human error related incidents within the participating organisation were due to commission. This provides a picture that the vast majority of human errors are as a result of a slip or lapse, whereby the person that the human error relates to performed a task but did so incorrectly rather than the incident occurring due to them not performing a task.

The most common primary elements of roles associated with human error related information security incidents within the public sector organisation were communications and administration.

Primary Element of the Role	**Frequency**
Administration	54
Communications	67
Computer End User	50
Data Entry	11
Document or Equipment Destruction	4
Email User	19
Filing	40
Human Resources	2
IT Support	27
Line Manager	14
Mobile Phone User	7
Total	**295**

Table 4 – Primary element of the role that is pertinent to the incident/human error

The most common specific activities that led to the incidents within the participating organisation were Sending an Email – 76 (25.5%), Posting Documents – 69 (23.2%), Data Filing – 52 (17.4%), and IT System Configuration, Administration, Development or Support – 22 (7.4%).

Specific Activity	**Count**
Accessing server room	1
Administration	1
Clearing screen of previous information	1
Communications to employer (post)	1
Communications to Service Desk (email)	34
Communications to sService Pprovider (post)	1
Communications to service users (phone)	1
Communications to service users (post)	14
Configuration of proxy services	1
CV Pprocedure	1
Data entry or modification	4
Data Ffiling	23
Data Ffiling - records update	11
Data filing - scanning	13
Data filing - scanning documents using reference numbers	5

Specific Activity	Count
Destruction of documents	4
Document ~~M~~management - ~~S~~service ~~U~~user ~~V~~verification	1
ID pass management	1
Instigate leavers procedure	7
IT ~~S~~support	2
IT ~~S~~system ~~A~~administration	4
IT ~~S~~system ~~C~~configuration	10
IT ~~U~~user	1
Leavers procedure	7
Manual correction of system reference number	1
Password reset	1
Password ~~S~~security and ~~M~~management	5
Placing a document in an envelope	23
Posting documents	53
Printing of documents	1
Publication of user guides	1
Raising leavers form	3
Recording caller details	1
Recording ~~S~~service ~~U~~user ~~D~~details	1
Safeguarding company equipment	7
Sending an email	42
System coding	1
Systems ~~D~~development	3

Specific Activity	Count
Update of records	3
Use of IT ~~S~~system - ~~P~~password ~~S~~haring	1
User was providing training to a client organisation	1
N/a - not task related	1
Total	**298**

Table 5 - Specific activity being performed that led to the incident/human error

6.2 Error Producing Condition results

The most common primary, secondary and tertiary EPCs within the participating organisation can be seen in Table 6.

	Error Producing Condition	Primary EPC Count	Secondary EPC Count	Tertiary EPC Count
1	EPC 2 - A shortage of time available for error detection and correction	141	4	1
2	EPC 7 - No obvious means of reversing an unintended action	74	3	0
3	EPC 11 - Ambiguity in the required performance standards	31	7	0
4	EPC 17 - Little or no independent checking or testing of output	15	16	10
5	EPC 1 - Unfamiliarity with a situation	1	0	0

	Error Producing Condition	Primary EPC Count	Secondary EPC Count	Tertiary EPC Count
	which is potentially important but which only occurs infrequently or which is novel			
6	EPC 12 - A mismatch between perceived and real risk	9	15	1
7	EPC 32 - Inconsistency of meaning of displays and procedures	4	0	0
8	EPC 6 - A mismatch between an operator's model of the world and that imagined by a designer	2	0	0
9	EPC 25 - Unclear allocation of function and responsibility	2	0	0
10	EPC 10 - The need to transfer specific knowledge from task to task without loss	1	0	0
11	EPC 13 - Poor, ambiguous or ill-matched system feedback	1	0	0
12	EPC 15 - Operator inexperience (e.g. a newly-qualified tradesman, but not an "expert")	1	0	0
13	EPC 16 - An impoverished quality of information conveyed by procedures	1	14	1

	Error Producing Condition	Primary EPC Count	Secondary EPC Count	Tertiary EPC Count
	and person/person interaction			
14	EPC 21 - An incentive to use other more dangerous procedures	1	0	0
15	EPC 23 - Unreliable instrumentation (enough that it is noticed)	1	0	0
16	EPC 26 - No obvious way to keep track of progress during an activity	1	1	0
17	EPC 34 - Prolonged inactivity or highly repetitious cycling of low mental workload tasks	0	66	4
18	EPC 3 - A low signal-noise ratio	0	57	0

Table 6 – Primary, secondary and tertiary EPCs

Finally the primary (most impacting), secondary and tertiary (least impacting) EPCs were totalled to give an overall view in the respective organisations as to the volume of EPCs selected that had a definite contributing factor to the information or cyber security incidents occurring. The results for the participating organisation are shown in table 7.

	Error Producing Condition	Count
1	EPC 2 - A shortage of time available for error detection and correction	146
2	EPC 7 - No obvious means of reversing an unintended action	77

	Error Producing Condition	Count
3	EPC 34 - Prolonged inactivity or highly repetitious cycling of low mental workload tasks	70
4	EPC 3 - A low signal-noise ratio	57
5	EPC 17 - Little or no independent checking or testing of output	41
6	EPC 11 - Ambiguity in the required performance standards	38
7	EPC 12 - A mismatch between perceived and real risk	25
8	EPC 16 - An impoverished quality of information conveyed by procedures and person/person interaction	16
9	EPC 32 - Inconsistency of meaning of displays and procedures	4
10	EPC 6 - A mismatch between an operator's model of the world and that imagined by a designer	2
11	EPC 25 - Unclear allocation of function and responsibility	2
12	EPC 26 - No obvious way to keep track of progress during an activity	2
13	EPC 1 - Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel	1
14	EPC 10 - The need to transfer specific knowledge from task to task without loss	1
15	EPC 13 - Poor, ambiguous or ill-matched system feedback	1
16	EPC 15 - Operator inexperience (e.g. a newly-qualified tradesman, but not an "expert")	1
17	EPC 21 - An incentive to use other more dangerous procedures	1
18	EPC 23 - Unreliable instrumentation (enough that it is noticed)	1

Table 7 – Total count of all EPCs identified

The results show that athe significant proportion of human error related incidents were due to a shortage of time available for error detection and correction, which was a factor in 61% of the reported human error related incidents. The results also indicate that there is an obligation for organisations to ensure employees are given opportunity to reverse or stop an unintended action. The organisations should also ensure that they are consciously aware of people processing confidential information whilst performing repetitious tasks.

6.3 Generic Task Type results

The most common GTT was E followed by D as shown in table 8. GTT E and D accounted for 89.9% of the reported and validated human error related incidents showing that reported incidents tended to relate to routine and simple tasks. Within the participating organisation, GTT M, a miscellaneous task selected if one of the other available GTTs did not appear to be relevant, was only selected 4 times from within 298 reported and validated human error related incidents. This supportsing the claim that HEART is an applicable tool within and information security setting.

	Generic task type	**Count**
1	GTT E - Routine, highly-practised, rapid task involving relatively low level of skill	169
2	GTT D - Fairly simple task performed rapidly or given scant attention	99

	Generic task type	Count
3	GTT B - Shift or restore system to a new or original state on a single attempt without supervision or procedures	20
4	GTT M - Miscellaneous task for which no description can be found	4
5	GTT A - Totally unfamiliar, performed at speed with no real idea of likely consequences	3
6	GTT F - Restore or shift a system to original or new state following procedures, with some checking	1
7	GTT G - Completely familiar, well-designed, highly practised, routine task occurring several times per hour, performed to highest possible standards by highly-motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids	1
8	GTT H - Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	1
9	GTT C - Complex task requiring high level of comprehension and skill	0

Table 8 – Generic Task Types

6.4 Statistical data results

In total there were 103 of the 322 private sector incidents which contained the required data to establish both the predicted and actual likelihood of reported incidents. The statistical data presented in Table 9, utilising mean averages

to three decimal places of the attained results for each GTT, indicates that the inbuilt HEART calculations do not align to the reported information security incidents due to the fact that the average actual likelihood was lower than the average nominal likelihood of failure in all cases.

Generic Task Type	Count of validated incidents	Average Nominal Likelihood of Failure	Average Nominal Likelihood of Failure Lower Bound	Average Nominal Likelihood of Failure Upper Bound	Average Actual Likelihood
GTT A	0				
GTT B	13	2.533	1.364392308	4.092176923	0.013278107
GTT C	0				
GTT D	55	0.727679025	0.485452684	1.05049808155	0.021062002
GTT E	31	0.193299355	0.068754774	0.434223548	0.00548064
GTT F	0				
GTT G	1	0.0044	0.001088	0.077	0.001096154
GTT M	3	0.330	0.088	1.210	0.015495726

Table 9 – Public sector predicted and actual likelihoods

7. Comparison with private sector results

Although it was proved in both public and private sector organisations that the majority of reported security incidents related to human error, there was a large difference in the percentages of human error. The private sector organisation recorded 51% of information security incidents as being due to

human error whereas the public sector organisation was 92.5%. A key difference between the organisations was the establishment of embedded information security policy across the whole public sector organisation as well as established and consistent incident reporting procedures. As the same level of information security incident management was not present across the much larger private sector organisation it is conceivable that not all information security incidents were reported to the central function despite both organisations leveraging definitions based upon ISO27001 [64] in order to define what constitutes an information security incident within policy.

One of the key general findings based upon comparison of the public and private sector organisations was the number of respective human error related incidents that pertained to omission or commission. Both organisations independently presented very similar findings. 256 (87.7%) of incidents within the public sector organisation and 84 incidents (90.3%) within the private sector organisation were due to commission. The percentages were very similar in both participating organisations (difference of 2.6%) showing that consistently incidents occur due to people performing a task incorrectly rather than not performing a task.

In addition to the direct mapping of recorded incidents to the HEART HRA technique, a number of other data elements were captured as it was felt that this could provide useful insight for this research and subsequent research. Therefore, it was decided to capture the job titles for each human error related incident to establish any trends or patterns. Very similar results were

ascertained from both participating organisations. The results showed that the vast majority of incidents pertained to administrative roles where there was a requirement to complete high volumes of repetitive tasks involving personal or confidential data.

The main similarity with both participating organisations was that 'administration' was the second most common primary element. It should be noted that both organisations have different business processes so this cannot be deemed a direct comparison but is useful information within their respective organisations. Another type of data captured during the case study outside of the direct mapping to HEART was identifying the tasks, processes or activities being performed that led to the incident occurring. There were no relationships identified between the organisations. Within the private sector organisation the most common tasks or processes were safekeeping of company materials and service setup, . ~~W~~whereas the most common within the public sector organisation were postal and email communications.

The next section focu~~s~~ses upon the direct mapping of all recorded incidents to the 38 ~~EPC's~~EPCs within the HEART HRA method [12]. EPC 38, age of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (sight, hearing, taste, smell or touch), was not used within the public sector organisation as it was felt by the organisation that this could be perceived as discriminatory and could not be acted upon. The private sector organisation did not request that EPC 38 be omitted. For each incident recorded, the respective business area

representative was required to select only ~~EPC's~~EPCs which definitely had an impact on the incident occurring. The business area representative was able to select from zero to a maximum of three ~~EPC's~~EPCs for each incident.

	Error Producing Condition	Primary EPC Count	Secondary EPC Count	Tertiary EPC Count
1	EPC 2 - A shortage of time available for error detection and correction	43	1	7
2	EPC 16 - An impoverished quality of information conveyed by procedures and person/person interaction	12	0	0
3	EPC 7 - No obvious means of reversing an unintended action	11	11	0
4	EPC 1 - Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel	4	0	1
5	EPC 11 - Ambiguity in the required performance standards	4	10	0
6	EPC 3 - A low signal-noise ratio	3	0	0
7	EPC 17 - Little or no independent checking or testing of output	3	0	1

Table 10 – Private sector organisation primary, secondary and tertiary EPCs

There was correlation witnessed with both organisations identifying that EPC 2, referring to a shortage of time available for error detection and correction, was the most common primary EPC~~,~~ and reason that it was felt the human error occurred which resulted in an information security incident. There was no relationship identified between the participating organisations with regard to the secondary ~~EPC's~~EPCs captured. A relationship was identified with regard to the tertiary ~~EPC's~~EPCs selected by both participating organisations as both selected EPC 2 and 7.

Finally the primary, secondary and tertiary ~~EPC's~~EPCs were totalled to give an overall view in the respective organisations as to the volume of ~~EPC's~~EPCs selected that had a definite contributing factor to the information security incidents occurring.

	Error Producing Condition	**Count**
1	EPC 2 - A shortage of time available for error detection and correction	51
2	EPC 7 - No obvious means of reversing an unintended action	22
3	EPC 11 - Ambiguity in the required performance standards	14
4	EPC 16 - An impoverished quality of information conveyed by procedures and person/person interaction	12
5	EPC 1 - Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel	5
6	EPC 17 - Little or no independent checking or testing of output	4
7	EPC 3 - A low signal-noise ratio	3

Table 11 – Private sector organisation total count of all EPCs identified

Therefore the significant proportion of human error related incidents were due to a shortage of time to perform the intended task. There was a strong correlation between public and private sector organisations. The most common two ~~EPC's~~EPCs were the same for both organisations (2 and 7) and of the most common seven ~~EPC's~~EPCs, both organisations had five that matched (2, 3, 7, 11, 17).

In terms of statistical comparison between the public and private sector organisations, the research has found correlations. The organisations could statistically be compared against GTTs B, D, E and G as they were selected by both organisations. The private sector average nominal HEART likelihood and average actual likelihood can be seen in table 12.

Generic Task Type	**Count of validated incidents**	**Average Nominal Likelihood of Failure**	**Average Nominal Likelihood of Failure Lower Bound**	**Average Nominal Likelihood of Failure Upper Bound**	**Average Actual Likelihood**
GTT A	1	4.950	3.150	8.730	0.0065769
GTT B	2	0.74988	0.4032	1.2096210	0.0021603
GTT C	0				
GTT D	35	0.243071	0.162047	0.351102	0.0109688
GTT E	2	0.0687508	0.0243628	0.1521893	0.004327
GTT F	3	0.124375	0.033	0.289875	0.160258

Generic Task Type	Count of validated incidents	Average Nominal Likelihood of Failure	Average Nominal Likelihood of Failure Lower Bound	Average Nominal Likelihood of Failure Upper Bound	Average Actual Likelihood
GTT G	39	0.004462	0.0010892	0.078077	0.000089
GTT M	0				

Table 12 – Private sector predicted and actual likelihoods

Within both organisations the average actual likelihood was lower than the average HEART nominal lower bound in all cases with the exception of GTT G for the public sector organisation and GTT F for the private sector organisation. However, there wasere only 1 public sector incident mapped to GTT G and 3 private sector incidents mapped to GTT F.

8. Discussion

8.1 Principle findings

Our research has found that the majority of incidents within the participating public sector organisation relate to human error. The research findings of the empirical case study has identified that the actual proportion of reported public sector information security incidents within the participating organisation that relate to human error was 92.5%. Also analysis of published incidents and breaches indicates that the proportion of UK public sector personal data human error related breaches is probably in excess of 96% [65].

The empirical research has found that the IS-CHEC technique is feasible for use for analysis of information security incidents within a public sector organisation from a qualitative perspective as all recorded human error related incidents were able to be mapped to the HEART GTTs and EPCs. However, from a quantitative perspective the HEART nominal likelihood lower bound calculations did not mirror, and were lower than, the actual likelihood of recorded incidents ~~as~~ with the exception of GTT G within the public sector organisation and GTT F within the private sector organisation.

8.2 Implications of the findings

Following this empirical study, further improvements to the IS-CHEC technique have been identified to enable greater applicability within the information security environment. These improvements relate to the in-built HEART component weightings in order to enable alignment between calculated and actual incident likelihoods. The presented improvements also relate to the usability of the IS-CHEC technique by people not experienced or qualified in human factor engineering. The research has also introduced positive implications for the participating public sector organisation in that they now have a detailed understanding of the main causes of their reported information security incidents. This detailed research has subsequently enabled the organisation to increase its information security resourcing and formally embed the IS-CHEC technique within their incident practices to actively address information security related human error on an ongoing basis.

8.3 Comparison with the literature

As presented within the related work section of the paper there is a diverse range of understanding relating to the proportions of human error related information security incidents. However, the actual volumes of human error related information security incidents are roughly in line with ~~the~~ ~~p~~Parsons [46] who claimed that 95% ~~percent~~ of incidents related to human error. The public sector organisation studies as part of this research found that 92.5% of incidents were human error related.

8.4 Validation against published public sector personal data breaches

In addition to the empirical case study, an analysis of published personal data breaches was performed [65] in order to obtain external validation of our results. The sources of this external validation were the ICO data breach trends website [66] and also the published NHS serious incidents requiring investigation (SIRI) 2 relating to Q3 2017 [67]. It was found that ~~it~~ human error was involved in possibly 96% of breaches and incidents for central government and 98% for local government and health sectors [65].

8.5 Limitations of the method

Some expected and unexpected limitations of the method were experienced which mirrored our research undertaken with a private sector organisation [12]. This included the retrospective assessment of the previously reported incidents. This activity required significant effort by the respective business area representatives to ascertain accurate facts and resulted in the mapping

of all incidents against the IS-CHEC tool taking considerably longer than intended. The mapping completion was undertaken over a period of ten months.

In addition, the public sector empirical case study and similarly the private case study both found that the information security leads tended not to weight the APOA in a pessimistic manner, as required by the HEART technique. Due to the use of percentages they were subconsciously aiming for the combined EPCs to total 100% despite this requirement being presented and documented within population procedures. This was not an expected limitation but has provided good information to enable further enhancement of the IS-CHEC tool.

Another unexpected limitation was the fact that the public sector organisation made a decision to exclude EPC 38 (Age of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (sight, hearing, taste, smell or touch)) as it was felt that this could be perceived as discriminatory and could not be acted upon.

9. Conclusions and Future Work

Based on the findings presented after analysis of the two case studies in public and private [12] sector organisations, it can be concluded that the proportions of human error are far higher than previously reported in most of the accepted literature. The research has concluded that the actual empirically tested validated volumes of human error information security incidents are very high and certainly aligning to the few empirical case studies

previously published in literature [46]. The participating public sector organisation established that 92.5% of its recorded information security incidents related to human error. There was a large difference in the numbers of reported information security incidents and also the percentages of human error related incidents recorded between the public (92.5%) and private (51%) sector organisations. A key difference between the organisations was the level of established information security maturity in terms of embedded policy, governance and procedures across ~~the~~ both entire organisations. The public sector organisation had established information security incident practices and governance whereas the private sector organisation only mirrored this in business areas that were required to meet external security standards. Therefore, future research should ascertain the impact organisational information security maturity has upon the reporting, recording and understanding of information security incidents.

The empirical study has found that the most common cause of human error that led to an information security incident within the participating public sector organisation was a lack of time for error detection and correction. This matches the findings from the equivalent research undertaken with a private sector organisation [12]. The second and third most common causes of human error were that there are no obvious means of reversing an unintended action and people performing repetitious tasks.

Based upon the research undertaken, there are a number of further enhancements that can be made to the IS-CHEC technique and tool. These

include supporting general understanding outside of the human factors community. Therefore, the terms used to describe the core HEART components are amended within the IS-CHEC technique. In addition, it is proposed that the GTT be mapped to specific tasks such as sending an email so that users can easily map tasks without having to understand terms which are not easily distinguishable. It is also proposed that the IS-CHEC nominal likelihood calculations be recalibrated following real-time analysis of information security incidents.

Wider analysis of public sector ~~security~~ personal data incidents and breaches by the ~~UK Information Commissioner's Office~~ICO reinforces this view and provides data that suggests that ~~that~~ the proportion of personal data breaches across the public sector is even higher still and in excess of 96% [65]. This wider analysis provides insight in that across private and public sectors the proportions of human error related personal data breaches are in excess of 90%.

Future work is planned to undertake a real-time six month action research cycle within both public and private sector organisations in parallel. This action research will apply the IS-CHEC technique and also begin to research the reduction element of the technique. This is intended to establish if the technique can be utilised to capture detailed information on human error related information security incidents and have a positive impact in terms of reducing and preventing human error related information security incidents.

Summary Points

What was already known on the topic

- Volumes of information security incidents were increasing
- Reported information security incidents included those which related to human error although the proportions were unknown
- There is a lack of information security focus on human error unlike other fields such as the safety field

What this study added to our knowledge

- It has been empirically established that human error proportions are higher than currently understood in the literature
- The majority of information security incidents pertain to human error and use of the IS-CHEC technique provides insight into the common causes of human error
- The IS-CHEC technique, as an information security adaptation of HEART, is applicable to the field of information security

References

[1] E. Bordessa, ICO data security statistics highlight need for increased staff awareness – IT Governance Blog, (2018). https://www.itgovernance.co.uk/blog/ico-data-security-statistics-

highlight-need-for-increased-staff-awareness/ (accessed March 17, 2018).

[2] Y. He, C. Johnson, Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template, Int. J. Med. Inform. 84 (2015) 941–949. doi:10.1016/J.IJMEDINF.2015.08.010.

[3] J. Rooksby, R.M. Gerry, A.F. Smith, Incident reporting schemes and the need for a good story, Int. J. Med. Inform. 76 (2007) S205–S211. doi:10.1016/J.IJMEDINF.2006.05.019.

[4] A. Heathcote, NHS Digital Information security incident: good practice guide - NHS Digital, 2017. https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/information-security-incident/good-practice-guide (accessed March 17, 2018).

[5] J.L. Fernández-Alemán, A. Sánchez-Henarejos, A. Toval, A.B. Sánchez-García, I. Hernández-Hernández, L. Fernandez-Luque, Analysis of health professional security behaviors in a real clinical setting: An empirical study, Int. J. Med. Inform. 84 (2015) 454–467. doi:10.1016/J.IJMEDINF.2015.01.010.

[6] R. Khajouei, R. Abbasi, M. Mirzaee, Errors and causes of communication failures from hospital information systems to electronic health record: A record-review study, Int. J. Med. Inform. 119 (2018) 47–53. doi:10.1016/J.IJMEDINF.2018.09.004.

[7] N.R. Samaranayake, S.T.D. Cheung, W.C.M. Chui, B.M.Y. Cheung, Technology-related medication errors in a tertiary hospital: A 5-year analysis of reported medication incidents, Int. J. Med. Inform. 81 (2012)

828–833. doi:10.1016/J.IJMEDINF.2012.09.002.

[8] S. Pelayo, S. Bernonville, Example of a Human Factors Engineering approach to a medication administration work system: Potential impact on patient safety, Int. J. Med. Inform. 79 (2010) e43–e57. doi:10.1016/J.IJMEDINF.2009.07.002.

[9] Big Brother Watch, Cyber attacks in local authorities, 2018. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/02/Cyber-attacks-in-local-authorities.pdf (accessed March 17, 2018).

[10] Ponemon Institute, Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview, 2017. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN& (accessed March 17, 2018).

[11] M. Evans, L.A. Maglaras, Y. He, H. Janicke, Human behaviour as an aspect of cybersecurity assurance, Secur. Commun. Networks. 9 (2016) 4667–4679. doi:10.1002/sec.1657.

[12] M. Evans, L. Maglaras, Y. He, H. Janicke, HEART-IS: A Novel Technique for Evaluating Human Error-Related Information Security Incidents, Comput. Secur. 80 (2019) 74–89.

[13] Big Brother Watch, A Breach of Trust, 2015. https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/08/A-Breach-of-Trust.pdf (accessed March 17, 2018).

[14] J. Rajamaki, J. Nevmerzhitskaya, C. Virag, Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF), in: 2018 IEEE Glob. Eng. Educ. Conf., IEEE, 2018: pp.

2042–2046. doi:10.1109/EDUCON.2018.8363488.

[15] S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, R.W. Boss, If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security, Eur. J. Inf. Syst. 18 (2009) 151–164. doi:10.1057/ejis.2009.8.

[16] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. 34(3) (2010) 523–548.

[17] A. Hovav, J. D'arcy, Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea, Inf. Manag. 49 (2012) 99–110. doi:10.1016/j.im.2011.12.005.

[18] P. Ifinedo, Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition Princely Ifinedo, Inf. Manag. 51 (2014) 69–79. doi:10.1016/j.im.2013.10.001.

[19] A.C. Johnston, M. Warkentin, FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY 1, Manag. Inf. Syst. Q. 34 (2010) 549–566.

[20] P.B. Lowry, G.D. Moody, Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies, Inf. Syst. J. 25 (2015) 433–463.

[21] P.B. Lowry, C. Posey, R.J. Bennett, T.L. Roberts, Leveraging fairness and reactance theories to deter reactive computer abuse following

enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust, Inf. Syst. J. 25 (2015) 193–230.

[22] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, A. Vance, What levels of moral reasoning and values explain adherence to information security rules? An empirical study, Eur. J. Inf. Syst. 18 (2009) 126–139. doi:10.1057/ejis.2009.10.

[23] P. Puhakainen, M. Siponen, Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, MIS Q. 34 (2010) 757–778. doi:10.2307/25750704.

[24] M. Siponen, A. Vance, Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, MIS Q. 34 (2010) 487–502. doi:10.2307/25750688.

[25] M. Siponen, M.A. Mahmood, S. Pahnila, Employees' adherence to information security policies: An exploratory field study, Inf. Manag. 51 (2014) 217–224. doi:10.1016/j.im.2013.08.006.

[26] M. Siponen, A. Vance, Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations, Eur. J. Inf. Syst. 23 (2014) 289–305. doi:10.1057/ejis.2012.59.

[27] Y. Chen, K. Ramamurthy, K.-W. Wen, Organizations' Information Security Policy Compliance: Stick or Carrot Approach?, J. Manag. Inf. Syst. 29 (2012) 157–188. doi:10.2753/MIS0742-1222290305.

[28] J.-Y. Son, Out of fear or desire? Toward a better understanding of

employees' motivation to follow IS security policies, Inf. Manag. 48 (2011) 296–302. doi:10.1016/j.im.2011.07.002.

[29] A. Anderson, B. Kirwan, B. Eargle, Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG), J. Assoc. Inf. Syst. 15 (2014) 679–722.

[30] A. Vance, P.B. Lowry, D. Egget, Using Accountability to Reduce Access Policy Violations in Information Systems, J. Manag. Inf. Syst. 29 (2013) 263–289.

[31] A. Vance, M. Siponen, S. Pahnila, Motivating IS security compliance: Insights from Habit and Protection Motivation Theory, Inf. Manag. 49 (2012) 190–198. doi:10.1016/j.im.2012.04.002.

[32] J. D'Arcy, T. Herath, A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings, Eur. J. Inf. Syst. 20 (2011) 643–658. doi:10.1057/ejis.2011.23.

[33] J.D.' Arcy, A. Hovav, D. Galletta, User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Inf. Syst. Res. 20(1) (2009) 79–98. doi:10.1287/isre.1070.0160.

[34] J. D'Arcy, T. Herath, M.K. Shoss, Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective, J. Manag. Inf. Syst. 31 (2014) 285–318. doi:10.2753/MIS0742-1222310210.

[35] T. Dinev, Q. Hu, The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies, J.

Assoc. Inf. Syst. 8 (2007) 386–408. doi:10.17705/1jais.00133.

[36] K.H. Guo, Y. Yuan, The effects of multilevel sanctions on information security violations: A mediating model, Inf. Manag. 49 (2012) 320–326. doi:10.1016/j.im.2012.08.001.

[37] K.H. Guo, Y. Yuan, N.P. Archer, C.E. Connelly, Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model, J. Manag. Inf. Syst. 28 (2011) 203–236. doi:10.2753/MIS0742-1222280208.

[38] T. Herath, H. Raghav Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, Eur. J. Inf. Syst. 18 (2009) 106–125. doi:10.1057/ejis.2009.6.

[39] T. Herath, H.R. Rao, Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, Decis. Support Syst. 47 (2009) 154–165. doi:10.1016/j.dss.2009.02.005.

[40] A.M.Y. Chu, P.Y.K. Chau, Development and validation of instruments of information security deviant behavior, Decis. Support Syst. 66 (2014) 93–101. doi:10.1016/j.dss.2014.06.008.

[41] H.G. Djajadikerta, S. Mat, R.T. Trireksani, Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research, Inf. Manag. 52 (2015) 1012–1024. doi:10.1016/j.im.2015.07.008.

[42] B.-Y. Ng, A. Kankanhalli, Y. Xu, Studying users' computer security behavior: A health belief perspective, Decis. Support Syst. 46 (2008)

815–825. doi:10.1016/j.dss.2008.11.010.

[43] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, N. Li, Enhancing security behaviour by supporting the user, Comput. Secur. 75 (2018) 1–9. doi:10.1016/j.cose.2018.01.016.

[44] H.A. Hamid, M.M. Yusof, N.R.S. Mohd Dali, Security compliance behaviour of SaaS cloud users: A pilot study, 12 (2017) 4150–4155. doi:10.3923/jeasci.2017.4150.4155.

[45] D.S. Wall, Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders, 2011. http://www.symantec.com/content/de/de/about/downloads/press/WP_Organizational_Security_and_the_InsiderThreat_Malicious_Negligent_and_Well-Meaning_FINAL.pdf (accessed March 17, 2018).

[46] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, T. Zwaans, The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Comput. Secur. 66 (2017) 40–51. doi:10.1016/j.cose.2017.01.004.

[47] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, The Human Factor of Information Security: Unintentional Damage Perspective, Procedia - Soc. Behav. Sci. 147 (2014) 424–428. doi:10.1016/J.SBSPRO.2014.07.133.

[48] A. Mahfuth, S. Yussof, A.A. Baker, N. Ali, A systematic literature review: Information security culture, in: 2017 Int. Conf. Res. Innov. Inf. Syst., IEEE, 2017: pp. 1–6. doi:10.1109/ICRIIS.2017.8002442.

[49] T. Halevi, N. Memon, J. Lewis, P. Kumaraguru, S. Arora, N. Dagar, F.

Aloul, J. Chen, Cultural and psychological factors in cyber-security, Proc. 18th Int. Conf. Inf. Integr. Web-Based Appl. Serv. 13 (2017) 43–56.

[50] C. Lee, C.C. Lee, S. Kim, Understanding information security stress: Focusing on the type of information security compliance activity, Comput. Secur. 59 (2016) 60–70. doi:10.1016/j.cose.2016.02.004.

[51] D. Basin, S. Radomirovic, L. Schmid, Modeling Human Errors in Security Protocols, in: 2016 IEEE 29th Comput. Secur. Found. Symp., IEEE, 2016: pp. 325–340. doi:10.1109/CSF.2016.30.

[52] A. AlHogail, Design and validation of information security culture framework, Comput. Human Behav. 49 (2015) 567–575. doi:10.1016/j.chb.2015.03.054.

[53] M.M. Yusof, J. Kuljis, A. Papazafeiropoulou, L.K. Stergioulas, An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit), Int. J. Med. Inform. 77 (2008) 386–398. doi:10.1016/J.IJMEDINF.2007.08.011.

[54] P.C. Cacciabue, G. Vella, Human factors engineering in healthcare systems: The problem of human error and accident management, Int. J. Med. Inform. 79 (2010) e1–e17. doi:10.1016/J.IJMEDINF.2008.10.005.

[55] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, Y. Xiang, Detecting and Preventing Cyber Insider Threats: A Survey, IEEE Commun. Surv. Tutorials. (2018) 1–1. doi:10.1109/COMST.2018.2800740.

[56] S. Kraemer, P. Carayon, Human errors and violations in computer and information security: The viewpoint of network administrators and

security specialists, Appl. Ergon. 38 (2007) 143–154. doi:10.1016/j.apergo.2006.03.010.

[57] I. Hwang, O. Cha, Examining technostress creators and role stress as potential threats to employees' information security compliance, Comput. Human Behav. 81 (2018) 282–293. doi:10.1016/j.chb.2017.12.022.

[58] J.T. Reason, Human error, Cambridge University Press, 1990.

[59] J.C. Williams, A User Manual for the HEART Human Reliability Assessment Method, (1992).

[60] Health and Safety Executive, Leadership and worker involvement toolkit Understanding human failure, 2012. http://www.hse.gov.uk/construction/lwit/assets/downloads/human-failure.pdf (accessed March 17, 2018).

[61] D. Embrey, Understanding Human Behaviour and Error, (2005). http://www.humanreliability.com/articles/Understanding Human Behaviour and Error.pdf (accessed March 17, 2018).

[62] J. Reason, Human error: models and management., BMJ. 320 (2000) 768–770. doi:10.1136/BMJ.320.7237.768.

[63] J. Bell, J. Holroyd, Review of human reliability assessment methods, Heal. Saf. Lab. (2009) 78. http://www.hse.gov.uk/research/rrpdf/rr679.pdf.

[64] The British Standards Institution, ISO/IEC 27001 - Information security management systems — Requirements, BSI, 2013. https://shop.bsigroup.com/ProductDetail?pid=000000000030347472&ut

m_source=google&utm_medium=cpc&utm_campaign=SM-STAN-PRM-CSR-iso27001-1810&creative=307410444133&keyword=%2Biso%2B27001&matchtype=b&network=g&device=c&gclid=EAIaIQobChMI1ovTo7_A3wIVLrvtCh0xi (accessed December 27, 2018).

[65] M. Evans, Y. He, I. Yevseyeva, H. Janicke, Analysis of published public sector information security incidents and breaches to establish the proportions of human error, in: Proc. 12th Int. Conf. Hum. Asp. Informarion Secur. Assur. - HAISA 2018, 2018: pp. 911–921.

[66] Information Commissioner's Office, Data security incident trends, 2018. https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

[67] Department of Health, IG Publications, 2017. https://www.igt.hscic.gov.uk/publications.aspx?tk=431547090342857&cb=1df2ac73-539f-a 43c4-9d06-96eff84c5eb5&lnv=14&clnav=YES (accessed March 17, 2018).

Appendices

Appendix A – IS-CHEC Mapping and Analysis Elements

Field	Description
Due to Human Error (y/n)	Establish if the incident is as a result of human error.
If not human error, is it human factor? (y/n)	If not due to human error is related to human factor. For example, due to malicious intent.

Field	Description
Specific activity being performed that led to the incident/human error	Establish the exact activity that was being performed such as sending an email, posting a document or updating a system.
Name of task or process being performed that led to the incident	As HEART is task based, the task associated with the incident is identified.
Time of day that the incident occurred	Based on recent amendments to HEART, 'Time of Day' has been added.
Number of times per week the task is performed	Capture frequency of task in order to compare with HEART probabilities.
Job title/role of the person the error pertains to	Capture the role related to this incident which has been deemed to be able to affect information security.

Field	Description
Primary element of the role that is pertinent to the incident/human error	Identify the primary element of the role which led to this incident. The options made available are: • Administration • Communications • Computer End User • Data Entry • Filing • Email User • Human Resources • IT Support • Line Manager • Mobile Phone User • Mobile Computer User • Senior Management • Remote/Home Worker • Document or Equipment Destruction
Other primary element of the role that is pertinent to the incident/human error	Opportunity to identify if another option is required other than those provided in the field above.
Error of commission or omission?	Capture if the incident as a result of not performing an activity or performing an activity incorrectly.

Field	Description
Generic task Type (GTT)	Generic task type within HEART that is applicable to the task being performed which resulted in the incident.
GTT Other (y/n)	Identify if there is no GTT within HEART which is applicable to this incident.
GTT Other Title	Select a title for a new information security GTT.
Primary Error Producing Condition (EPC)	Primary error producing condition that caused the incident.
% Primary EPC Assessed Proportion of Affect (APOA)	The assessed proportion of effect the EPC had on this incident (%).
Secondary Error Producing Condition (EPC)	Secondary error producing condition that caused the incident.
% Secondary EPC Assessed Proportion of Affect (APOA)	The assessed proportion of effect the EPC had on this incident (%).
Tertiary Error Producing Condition (EPC)	Tertiary error producing condition that caused the incident.

Field	Description
% Tertiary EPC Assessed Proportion of Affect (APOA)	The assessed proportion of effect the EPC had on this incident (%).
EPC Other (y/n)	Identify if there is no EPC within HEART which is applicable to this incident.
EPC Other Title	Select a title for a new information security EPC.
Data Validated	Establish if the data submitted could be confirmed as being validated by the researcher and participating organisation.

Table A1 – IS-CHEC mapping element

Field	Description
Nominal Unreliability	In-built HEART nominal unreliability associated with each GTT.
Nominal Unreliability Lower Bound	In-built HEART nominal unreliability lowest value within the techniques range associated with each GTT.
Nominal Unreliability Upper Bound	In-built HEART nominal unreliability highest value within the techniques range associated with each GTT.
Primary EPC APOA Decimal	Convert the recorded percentage to a decimal to enable calculations to be performed.
Primary EPC Strength	In-built HEART value/strength assigned to each EPC

Field	Description
Secondary EPC APOA Decimal	Convert the recorded percentage to a decimal to enable calculations to be performed.
Secondary EPC Strength	In-built HEART value/strength assigned to each EPC
Tertiary EPC APOA Decimal	Convert the recorded percentage to a decimal to enable calculations to be performed.
Tertiary EPC Strength	In-built HEART value/strength assigned to each EPC
Primary EPC Assessed Affect	In-built HEART Calculation establishing the effect of each identified EPC. Calculation uses the EPC strength and APOA. =(Primary EPC Strength-1)*Primary EPC APOA Decimal+1
Secondary EPC Assessed Affect	In-built HEART Calculation establishing the effect of each identified EPC. Calculation uses the EPC strength and APOA.
Tertiary EPC Assessed Affect	In-built HEART Calculation establishing the effect of each identified EPC. Calculation uses the EPC strength and APOA.

Field	Description
Nominal Likelihood of Failure	Nominal probability that is employed to characterise the general likelihood of task failure based on the in-built HEART calculation. =Nominal Unreliability*Primary EPC Assessed Affect*Secondary EPC Assessed Affect*Tertiary EPC Assessed Affect
Nominal Likelihood of Failure Lower Bound	Nominal lowest value probability based on the HEART ranges that is employed to characterise the general likelihood of task failure based on the in-built HEART calculation. =Nominal Unreliability Lower Bound*Primary EPC Assessed Affect*Secondary EPC Assessed Affect*Tertiary EPC Assessed Affect
Nominal Likelihood of Failure Upper Bound	Nominal highest value probability based on the HEART ranges that is employed to characterise the general likelihood of task failure based on the in-built HEART calculation. =Nominal Unreliability Upper Bound*Primary EPC Assessed Affect*Secondary EPC Assessed Affect*Tertiary EPC Assessed Affect

Field	Description
Number of times the task is performed per annum	Number of times that the particular task that was being performed and led to the incident is performed each year. =Number of times per week the task is performed *52
Number of reported incidents	Number times this particular type of incident occurred in a year. The population of this field is completed manually based on review of all incidents.
Actual Likelihood	Calculation based upon the number of times the task is performed and the recorded number of incidents in a year. =Number of reported incidents/Number of times the task is performed per annum
Actual Likelihood Calculated (Y/N)	Confirmation that all required data has been captured to enable the actual likelihood to be calculated.

Table A2 – IS-CHEC analysis element

CONFLICT OF INTERESTS

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

AUTHOR STATEMENT

Date: 23 Sep 2018

Dear Editors of International Journal of Medical Informatics,

I would like to submit the attached manuscript to be considered for possible publication in the International Journal of Medical Informatics.

We declare that this manuscript has not been published and is not currently being considered for publication elsewhere. We confirm that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed. We further confirm that the order of authors listed in the manuscript has been approved by all of us.

We confirm that we have given due consideration to the protection of intellectual property associated with this work and that there are no impediments to publication, including the timing of publication, with respect to intellectual property.

We understand that the Corresponding Author is the sole contact for the Editorial process (including Editorial Manager and direct communications with the office). She is responsible for communicating with the other authors about progress, submissions of revisions and final approval of proofs.

Author list and corresponding author

Mark Evans
Ying He, ying.he@dmu.ac.uk ***(Co-responding Author)***
Iryna Yevseyeva
Leandros Maglaras,
Helge Janicke

School of Computer Science and Informatics, De Montfort University

SUMMARY TABLE

What was already known on the topic

- Volumes of information security incidents were increasing in Healthcare
- Reported information security incidents included those which related to human error although the proportions were unknown
- There is a lack of information security focus on human error unlike other fields such as the safety field

What this study added to our knowledge

- This study has empirically established that human error proportions are higher than currently understood in the literature
- The majority of information security incidents pertain to human error and use of IS-CHEC provides insight into the common causes of human error
- IS-CHEC, as an information security adaptation of HEART, is applicable to the field of information security in a participating public sector organisation providing healthcare services